

REMARKS

Applicants have studied the Office action dated June 4, 2004, and have made amendments to the claims. Claim 1 has been amended. No new matter has been added. It is submitted that the application, as amended, is in condition for allowance. Reconsideration is respectfully requested.

Rejections under 35 U.S.C. § 103

Claims 1-6 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Adams et al., "Internet X.509 Public Key Infrastructure Time Stamp Protocol (TSP) <draft-ietf-pkix-time-stamp-08.txt>", June 2000 (Adams et al.). This rejection is respectfully traversed.

With regard to claim 1, Adams et al. discloses a method of providing a time stamping service which performs a time stamping operation by verifying whether a TimeStampResp packet itself is altered or not. In contrast, the method of the present invention performs a time stamping operation by verifying current time (genTime) under the assumption that a time stamping response (TimeStampResp) packet itself was not altered.

Furthermore, Adams et al. does not disclose a step of setting client's clock such that it is coincident with a result verified by a requester. Although Adams et al. discloses the steps of receiving a time stamping service from the TSA and verifying validity of the TSA, Adams et al. does not teach or suggest a step of setting client's terminal system clock based on a result generated after verifying an electronic signature value. In view of the above, it is respectfully submitted that claim 1 be allowed.

With regard to claim 2, the Examiner rejects the claim because Adams et al. discloses the step of generating a random number and setting it to a nonce value of a time stamping request (TimeStampReq). However, Adams et al. does not teach or suggest a hashing technique that hashes only a genTime generated by the TSA, based on a nonce value by a requester. The method according to the present invention performs an operation to check whether a TimeStampResp packet itself is altered or not. Only a genTime generated by the TSA is hashed using a nonce value generated

by a requester. A result of the hashing is stored in a corresponding field of a MacInfo structure. The result of the hashing contained in a TimeStampResp is transmitted to the requester. The requester performs a validation or verification operation with respect to the TimeStampResp. After, the requester authenticates and verifies the received TimeStampResp. The requester then confirms whether the genTime is altered or not based on a nonce value stored in the MacInfo structure and in a local storage of the requester. If the genTime is determined not to be altered, then a time setting operation is performed with respect to the client's terminal system.

In contrast, Adams et al. does not teach or suggest techniques for hashing only genTime using a nonce value, for defining a MacInfo structure using a result value of the hashing to store corresponding values associating therewith, and using the corresponding values to an extension field of the TimeStampResp. Although Adams et al. and the present invention are related to a time stamping method for electronic documents using a TimeStampReq and a requester, detailed techniques are unobviously different from each other. In view of this, Applicants respectfully submit that claim 2 be allowed.

With regard to claim 4, the steps of using a MAC value and verifying electronic signatures disclosed in Adams et al. serve only to check alteration with respect to a TimeStampResp packet. In contrast, the present invention verifies a genTime using a MacInfo structure and a nonce value under the assumption that the TimeStampResp packet itself was not altered. Accordingly, if the TimeStampResp packet itself discriminated to be altered by the technique of Adams et al. were applied to the present invention, the genTime would not be reliable. Therefore, Adams et al.'s technique is impossible to apply to the present invention. In view of this, Applicants respectfully submit that claim 4 be allowed.

With regard to claims 5 and 6, the Examiner states that Adams et al. teaches verifying the Time Server Authority's certificate validity using a Certificate Revocation List. In response, Applicants respectfully submit that Adams et al. checks whether a certificate is revoked using alteration of a TimeStampReq packet itself. In contrast, the present invention serves to verify genTime using the MacInfo structure and a nonce value, and to determine validity of a certificate revocation list.

Furthermore, claim 6 provides for setting the client's terminal system time using the genTime extracted from the TimeStampResp in a state that the genTime has been verified using the MacInfo structure and a nonce value. However, such a feature is neither taught nor suggested in Adams et al. Thus, although both Adams et al. and the present invention are related to time stamping technology, and include or use some part of the conventional time stamping standard specification, detailed operations to provided time stamping service between the present invention and Adams et al. are unobviously different from each other.

Additionally, the method of the present invention increases security when performing a verification step, unlike Adams et al. For the foregoing reasons, it is respectfully submitted that claims 5 and 6 be allowed.

Claims 1-6 were rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,728,880 to Sites (Sites) in view of U.S. Patent No. 6,314,517 to Moses (Moses). This rejection is respectfully traversed.

Sites relates to a method and apparatus for providing a trusted time. Specifically, a first local time from a computer is sent to a trusted server. Trusted time data protected by encryption or a digital signature is received from the trusted server. The trusted time data is stored on the computer and the validity of the trusted time is checked. The trusted time data is used on the computer to compute a trusted time corresponding to a local time.

Moses relates to a method and system for notarizing digital data, such as digital signature data. Specifically, the system determines a client compromised distribution latency period prior to authenticating the digital data. Upon receiving a notarization request, the system and method stores the digital data for notarization and holds the evidence or digital data for the latency period and as such waits to notarize the digital data in response to the client compromise distribution latency period.

In contrast, the present invention provides that when a requestor requests a time stamping service of the time stamping server, a nonce value is generated and a getBaseTime value is set in a predefined requestType parameter so as to inform the server that a corresponding message is a request for setting the client's system clock. Further, when a time stamping server (TSA) generates a response message in

response to a time stamping service requested by a requestor and transmits it to the requester, the method of the present invention generates a TimeStampResp based on a MacInfo structure, and enables the requester to use the MacInfo structure. Also, when the requester receives the response message from the TSA, and verifies the integrity thereof, the method of the present invention extracts the genTime, forms a MacInfo structure, calculates a MAC value therefrom, and determines whether the genTime is altered based on respective comparing steps.

Applicants respectfully submit that Sites and Moses either alone or in combination do not teach or suggest what is provided for in the present invention. Sites does not teach or suggest using a MacInfo structure for generating a TimeStampResp in the TSA and for calculating the MAC value in the requester. Here, the MacInfo structure is defined by combining a genTime, a nonce value and an algorithm identification such that a client's system clock is set using the time stamping protocol. Moses does teach or suggest using a MacInfo structure at all. Moreover, Moses does not teach or suggest a getBaseTime added in the requestType parameter. In view of the above, Applicants respectfully request that claims 1-6 be allowed over Sites and Moses.

CONCLUSION

In light of the above remarks, Applicants submit that the present Amendment places all claims of the present application in condition for allowance. Reconsideration of the application, as amended, is requested.

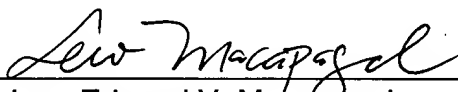
No amendment made was related to the statutory requirements of patentability unless expressly stated herein; and no amendment made was for the purpose of narrowing the scope of any claim, unless Applicant has argued herein that such amendment was made to distinguish over a particular reference or combination of references.

If for any reason the Examiner finds the application other than in condition for allowance, the Examiner is requested to call the undersigned attorney at the Los Angeles, California, telephone number (213) 623-2221 to discuss the steps necessary for placing the application in condition for allowance.

Respectfully submitted,

Lee, Hong, Degerman, Kang & Schmadeka

Date: October 4, 2004

By: 
Lew Edward V. Macapagal
Registration No. 55,416
Attorney for Applicant(s)

Customer No. 035884

Lee, Hong, Degerman, Kang & Schmadeka
801 S. Figueroa Street, 14th Floor
Los Angeles, California 90017
Telephone: 213-623-2221
Facsimile: 213-623-2211